

自動運転システムへのSTPA試行事例 ～JASPAR機能安全WG活動成果紹介～



*Japan
Automotive
Software
Platform
and
Architecture*

2018.12.4

JASPAR 機能安全WG

技術アドバイザー

STAMP/STPAチームリーダー

主査

宮崎 義弘

(日立オートモティブシステムズ(株))

橋本 岳男

(株)日立産業制御ソリューションズ

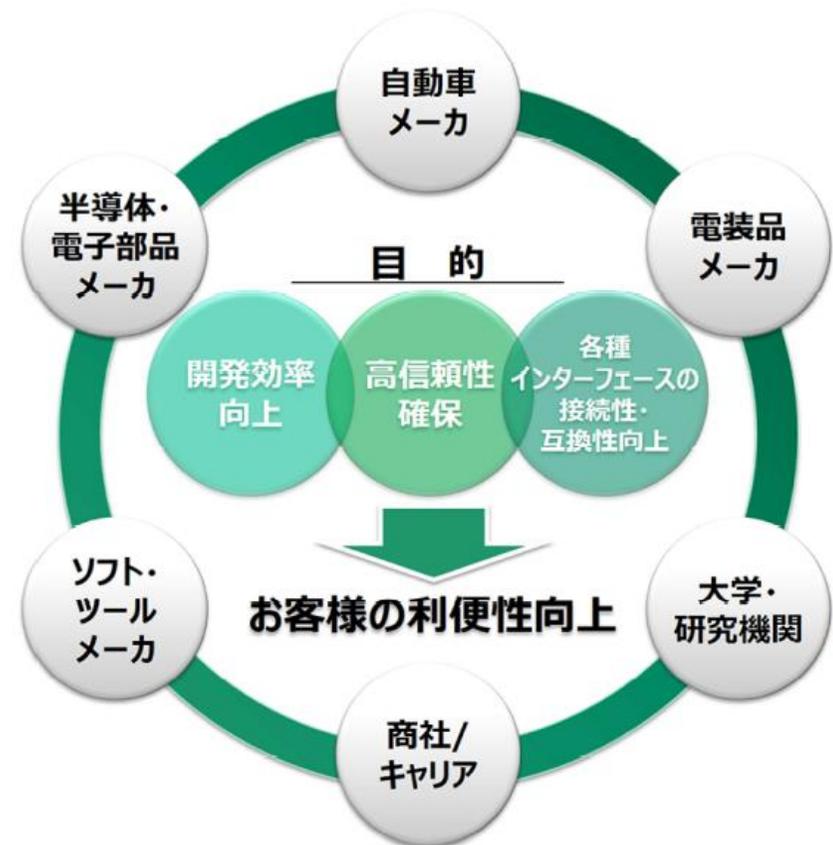
岡田 学

(日産自動車(株))

- (1) JASPAR機能安全WGの全体活動
- (2) STAMP/STPAチーム活動と事例拡充ガイド概要
- (3) 試行対象システム (自動運転システム)
- (4) STPA試行事例 (自動運転システム)
- (5) ライフサイクルに対しての試行
- (6) まとめ

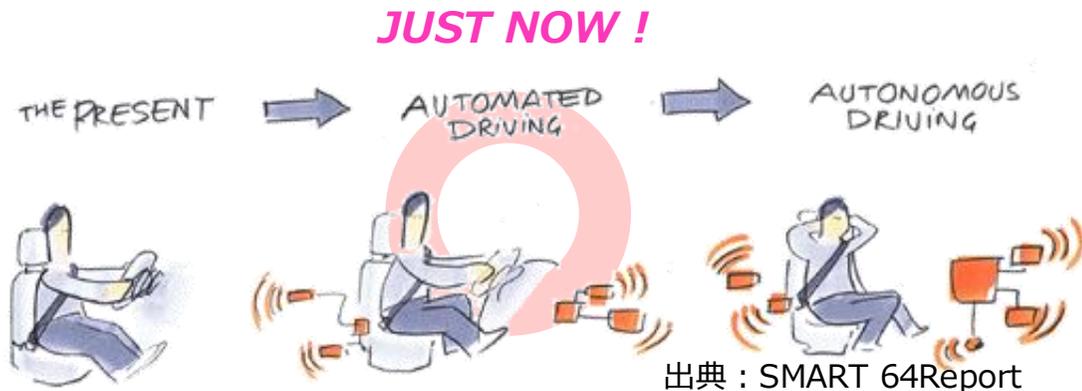
- (1) JASPAR機能安全WGの全体活動
- (2) STAMP/STPAチーム活動と事例拡充ガイド概要
- (3) 試行対象システム (自動運転システム)
- (4) STPA試行事例 (自動運転システム)
- (5) ライフサイクルに対しての試行
- (6) まとめ

- ◆団体名：一般社団法人JASPAR（Japan Automotive Software Platform and Architecture）
- ◆設立：2004年 ◆会員数：180社（2018年4月）
- ◆設立背景：高度化・複雑化する車載電子制御システムのソフトウェアやネットワークの標準化及び共通利用による、開発の効率化と高信頼性確保を目指す。
- ◆活動概要：
自動車メーカー、電装品メーカー、半導体・電子部品メーカー、ソフト・ツールメーカー、商社/キャリアの各業種、大学・研究機関から技術者が参画し、海外・国内の関連団体との協調の下、車載ネットワーク、ソフトウェア、情報セキュリティにおける標準化を推進する。
- ◆ミッション：
自動車の進化に伴うカーエレクトロニクス領域での将来の共通課題を特定し、その解決のための標準化活動に取り組み、自動車産業全体の公正な競争基盤の創造・開発の生産性向上と技術発展を促進する。
- ◆公開HP：<https://www.jaspar.jp/>





運転自動化レベルの進化



- ポイント
- 人-システムの運転役割交代へ
 - システムの前提が変更
 - 非故障の安全影響がますます重要

規格の変化

更新 ISO 26262: 2018(第2版)

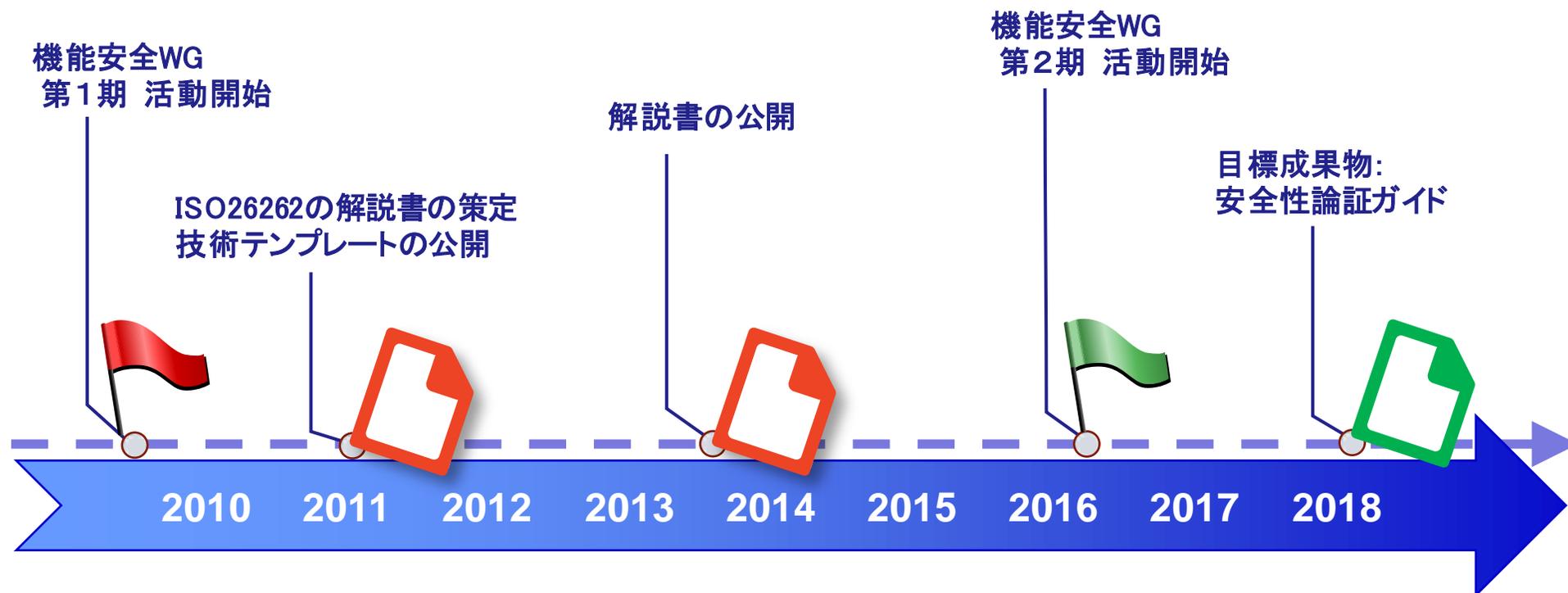
2018年発効予定
危険源の要因:
ランダム故障
システムティック故障

新規 SOTIF ISO/PAS 21448

2018年発効予定
危険源の要因:
性能限界
ミスユース

SOTIF: Safety Of The Intended Functionality

故障だけでなく非故障への対応に向け活動拡大 (System Safety視点)



◆機能安全WG 第2期（16年度～）の活動目標

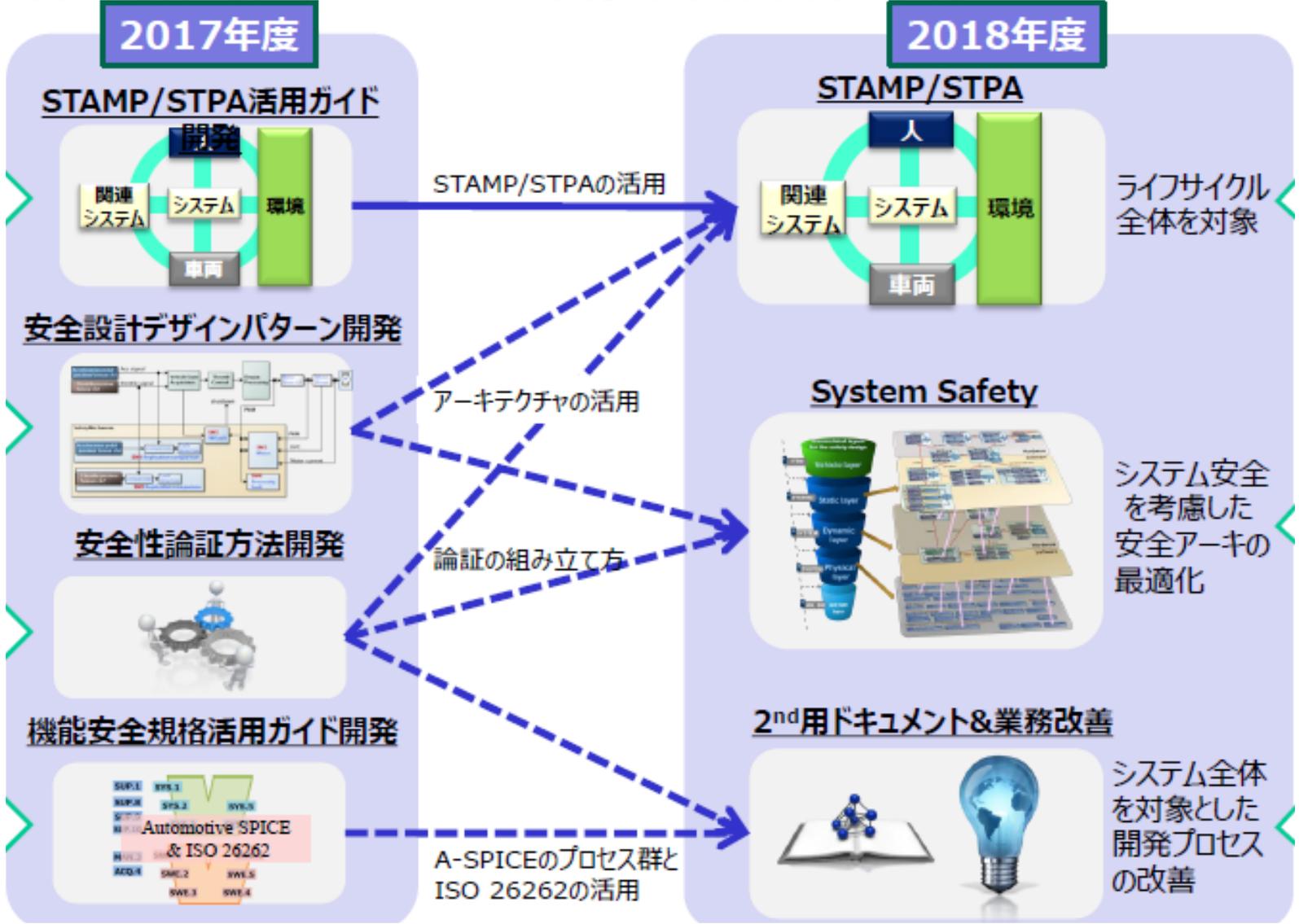
【目的】 機能安全設計における安全性論証を効果的・効率的にする

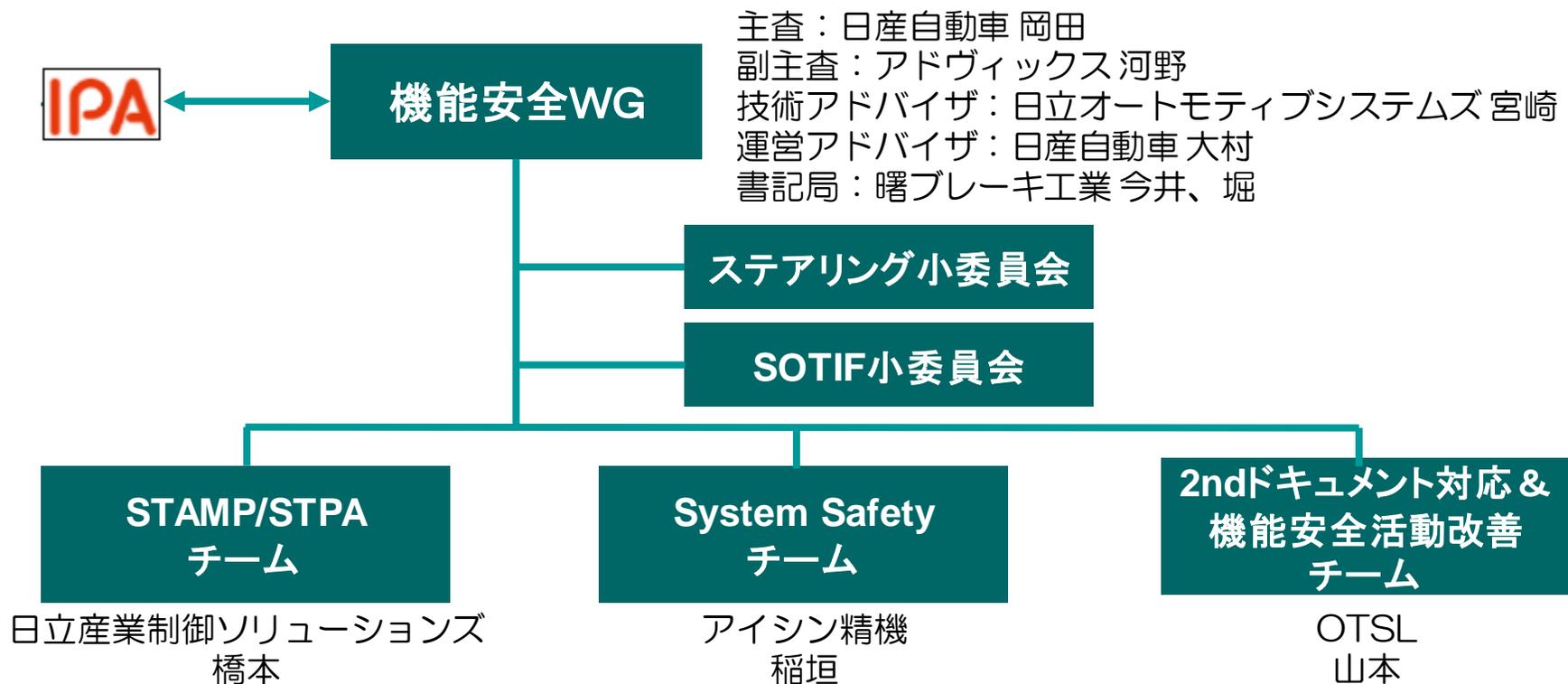
【成果物】 安全性論証ガイド

- 例) ・STAMP/STPA活用ガイド (自動車編)
・安全設計デザインパターン活用ガイド
・効果的な安全論証のための導入ガイド
・ソフトウェアパーティショニングガイド etc.

課題点に対する
技術の深堀

17年度の成果を引き継ぎ、18年度は3チーム体制でステップアップを図る





WG参加企業(18年度) 43社 (※50音順、敬称略、2018年11月)

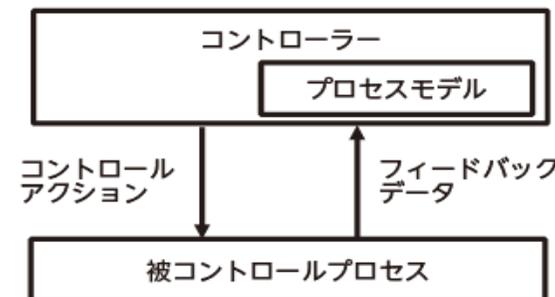
アイシン・エイ・ダブリュ(株)、アイシン精機(株)、曙ブレーキ工業(株)、(株)アドヴィックス、アルプス電気(株)、
 ヴィオニアジャパン(株)、ヴィオニア日信ブレーキシステムジャパン(株)、(株)ヴィッツ、(株)エクスマーション、SCSK(株)、
 (株)OTSL、(株)オーバス、オムロンオートモティブエレクトロニクス(株)、カルソニックカンセイ(株)、
 (株)ジェイテクト、シヤトコ(株)、スズキ(株)、住友電装(株)(住友電工Gr)、(株)チェンジビジョン、(株)デンソー、(株)デンソーテン、
 (株)東海理化、東芝デバイス&ストレージ(株)、東芝デジタルソリューションズ(株)、東芝情報システム(株)、トヨタ自動車(株)、
 (株)豊田自動織機、日産自動車(株)、日本アイ・ビー・エム(株)、日本ケイデンス・デザイン・システムズ社、
 日本精工(株)、日本電産エレシス(株)、パナソニック(株)、日立オートモティブシステムズ(株)、
 (株)日立産業制御ソリューションズ、(株)富士通ビー・エス・シー、古川AS(株)、ベクター・ジャパン(株)、ボッシュ(株)、
 (株)本田技術研究所、(株)村田製作所、三菱電機(株)、矢崎総業(株)、学会会員(IPA田丸様、IPA石井様)

- (1) JASPAR機能安全WGの全体活動
- (2) STAMP/STPAチーム活動と事例拡充ガイド概要**
- (3) 試行対象システム (自動運転システム)
- (4) STPA試行事例 (自動運転システム)
- (5) ライフサイクルに対しての試行
- (6) まとめ

マサチューセッツ工科大学(MIT)のNancy G Leveson教授によって提唱されたシステム安全分析手法

◆ STAMP (Systems Theoretic Accident Model and Processes) :
システム理論に基づくアクシデントモデル

システムの安全性は構成要素の相互作用から創発される。現代のシステムのアクシデントの多くは、システム構成要素の故障によって起きるのではなく、システムの中で安全のための制御を行う要素(コントローラ: Controller)と制御される要素(被コントロールプロセス: Controlled Process)の相互作用が働かないことによって起きる



◆ STPA (System Theoretic Process Analysis) :
STAMP アクシデントモデルを前提として、システムのハザード要因を分析する安全解析手法

STPA の手順の概要

- 1st Step : 解析目的を定義
- 2nd Step : コントロールストラクチャをモデル化
- 3rd Step : 非安全なコントロールアクション(UCA)を識別
- 4th Step : 損失シナリオを識別

注意:
本発表資料において、STPA手順のステップ番号は、STPA Handbook(MIT発行)に準拠した。

出典: はじめてのSTAMP/STPA IPA発行 <http://www.ipa.go.jp/sec/reports/20160428.html>
STPA Handbook MIT発行 http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

■ 高機能化/複雑化する分析対象の安全分析を補強



- 総合的な視点へ
- 安全分析範囲の拡張
- 検討過程の可視化による論証性向上

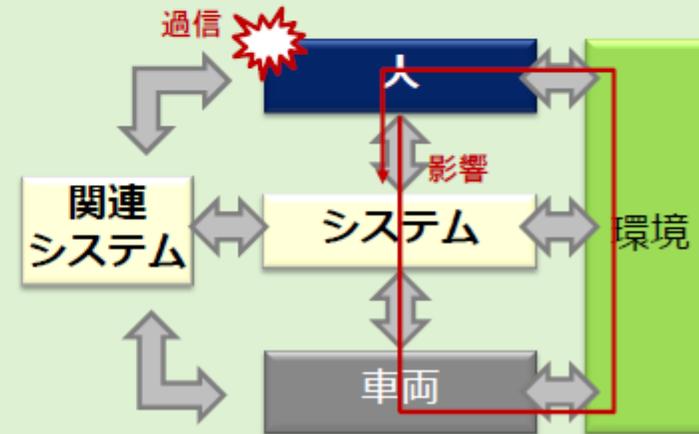
従来手法

システムを中心に周辺の影響を想像
→検討漏れ、手戻り発生



STAMP/STPA

全体視点でシステム周辺の相互作用を分析
→検討の網羅性向上、分かり易い説明



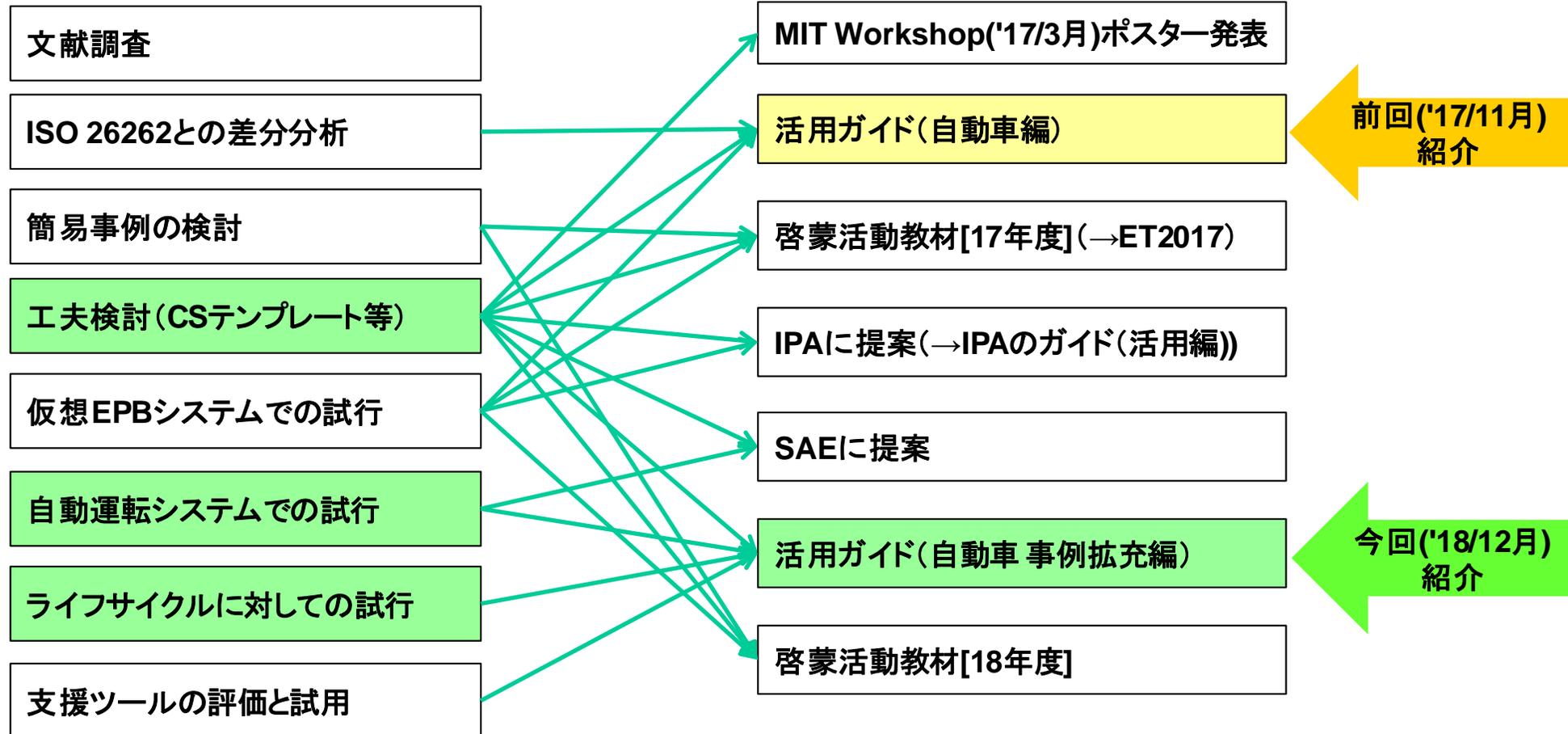
◆参加メンバー（18年度） 20社 （※50音順、敬称略、2018年11月）

アイシン・エイ・ダブリュ(株)、曙ブレーキ工業(株)、(株)アドヴィックス、(株)ヴィッツ、(株)エクスモーション、(株)OTSL、オムロンオートモーティブエレクトロニクス(株)、シヤトコ(株)、独立行政法人 情報処理推進機構(IPA)、スズキ(株)、(株)チェンジビジョン、(株)デンソーテン、東芝デバイス&ストレージ(株)、トヨタ自動車(株)、日産自動車(株)、日立オートモティブシステムズ(株)、(株)日立産業制御ソリューションズ、(株)富士通ビー・エス・シー、(株)本田技術研究所、三菱電機(株)



チーム活動

成果物の発行・情報発信



CS: Control Structure
EPB: Electric Parking Brake

ガイド名称：**安全性論証に使うSTAMP／STPA ～自動車 事例拡充編～**

- 自動運転システム(Lvl3)の分析事例として纏める
- ライフサイクルに対して分析範囲を拡大した内容も含める
- 支援ツールの試用例も含める



目次

1. 本書の位置付け.....	
2. 自動運転システムにおけるドライバとの相互作用の分析事例.....	
2.1. 事例選定の背景.....	
2.2. 本書で取り扱う事例の対象システム.....	
2.3. 想定トラブル事例.....	
2.4. コントロールアーキテクチャテンプレートの選定.....	
2.5. 第1ステップ 解析目的を定義.....	
2.6. 第2ステップ コントロールストラクチャをモデル化.....	
2.7. 第3ステップ 非安全なコントロールアクションを識別.....	
2.8. 第4ステップ 損失シナリオを識別.....	
2.9. 適用結果.....	
2.10. 各社の分析事例.....	
3. 自動運転システムにおける製品ライフサイクルに着目した分析事例.....	
参考文献.....	

- (1) JASPAR機能安全WGの全体活動
- (2) STAMP/STPAチーム活動と事例拡充ガイド概要
- (3) 試行対象システム (自動運転システム)**
- (4) STPA試行事例 (自動運転システム)
- (5) ライフサイクルに対しての試行
- (6) まとめ

車両レベルで実現したい目的・機能

- ・目的：日本の高速道路または自動車専用道路で、自動運転(Lvl3)を可能とする。
ドライバは運転以外のことをしてもよい。
また、ドライバは運転介在(オーバーライド)をしてもよい。

・機能：

(1)自動運転モード：

システムは自動車を目的地に向けて自動操縦する。自動運転モード時の機能は以下である。

- 通常走行(車線キープし法定速度で定速走行)
- 前方車追従走行
- 前方車追い越し走行
- オーバーライド
- 緊急時切替(システムの故障や性能限界時)
- 目的地設定(地図情報を使用し設定する)

(2)手動運転モード

システムは自動車をドライバの手動運転操作に従って操縦する。
ドライバの手動運転操作に従った走行

「クルマと人」に着目した安全分析 ⇒ その視点に関連する仕様を記載

1. 自動運転モード作動条件(AND条件)
 - ・ 高速道路または、自動車専用道路を走行時(標識認識と地図情報から判断)
 - ・ 自動運転作動スイッチを押下
2. 自動運転モード解除条件(OR条件)
 - ・ 目的地到着時にドライバがテイクオーバーを許可
 - ・ ドライバの操作によるオーバーライド
 - ・ ドライバが自動運転システム解除スイッチを押下
 - ・ 緊急時(自動運転システム継続不可時)にドライバがテイクオーバーを許可

<途中省略>

5. オーバーライド

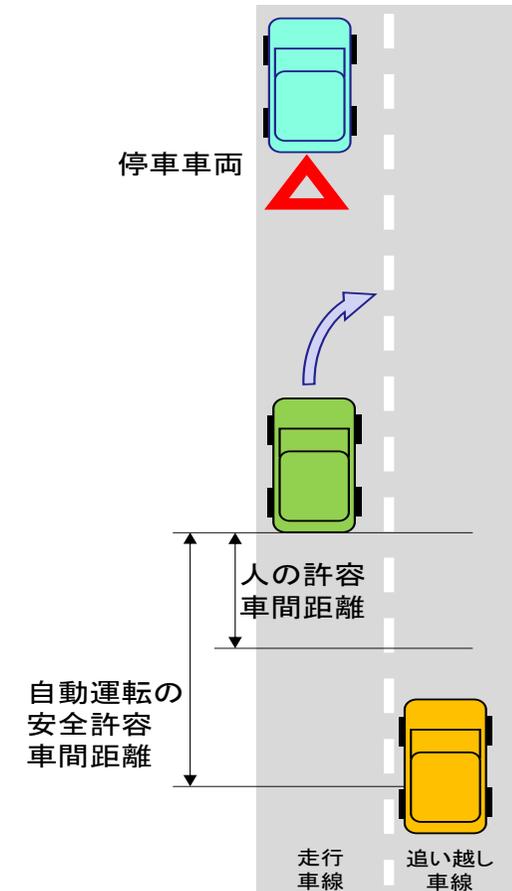
- (1)ドライバがステアリング又は、アクセル、ブレーキの操作を行う。また、ドライバがオーバーライドを行う意思があることの判別をする為に、ステアリング又は、アクセル、ブレーキ操作をある程度の操作力(**N・m)で一定時間継続(**s)することとする。
- (2)オーバーライド可能条件は以下
 - ・ステアリング操作:ステアリング操作方向に車両、または自車両を追い越し中の車両が無い場合
 - ・アクセル操作:(記載省略) ・ブレーキ操作:(記載省略)
- (3)オーバーライド不可時は、操作個所に反力を発生させドライバの操作を無効化する
- (4)オーバーライドした場合は、自動運転モードから手動運転モードに切り替わる

<以下省略>

想定トラブルの内容

ステアリング操作に対する、人(ドライバ)とシステム(自動運転システム)との競合トラブル

- (1) 自車は、高速道の走行車線を高速で走行中
- (2) 前方に停止した車両(または低速走行の車)を発見
- (3) 追い越し車線の後方に別の走行車を認知
- (4) ドライバは、追い越し車線に車線変更しようと、追い越し車線側にハンドルを操作
(追い越し車線の後方の走行車までは距離が十分あると判断)
- (5) 自動運転システムは、ドライバの追い越し車線側への車線変更操作を阻止
(追い越し車線の後方の走行車までは距離が不足と判断)
- (6) ドライバは、追い越し車線に車線変更しようと、さらに強く、追い越し車線側にハンドルを操作
- (7) 追い越し車線の後方の走行車がたまたま減速した(速度を緩めた)
- (8) 自動運転システムは、追い越し車線側への車線変更操作の阻止を解除
- (9) ドライバは、『さらに強く、追い越し車線側にハンドルを操作』としていたため、急な追い越し車線側への車線変更操作によって、車両が追い越し車線を越えて中央分離帯に衝突



想定トラブルの設定目的

STAMP/STPAのメリットを例示するために、相互作用によって発生しそうなトラブル例を想定し、STAMP/STPAにより同トラブルをシステムチェックに導出できるかに焦点を当て試行する。

想定トラブルの選定背景

特に自動運転Level3では、システムによる自動運転、または、ドライバによる手動運転により車両を制御する権限が状況により変化するため、人とシステムとの競合が大きな関心事となる。

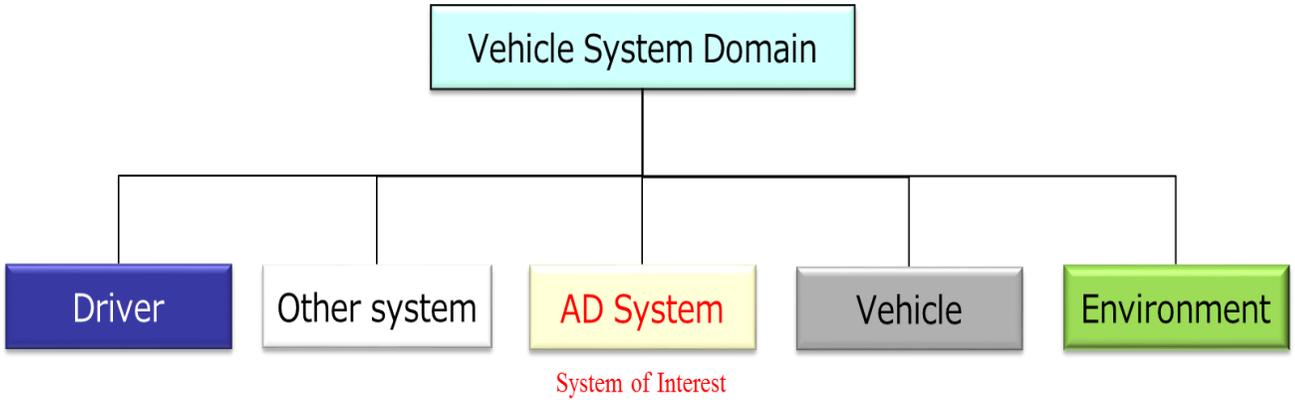
例えば、ドライバが自動運転システムに対しオーバーライドを要求時に、安全にオーバーライドできないとシステムが判断する場合は、『オーバーライド要求を拒否する』という安全機構が既に入っているシステムに対して、人とシステムの競合により非安全な状態になるかもしれない。そのようなケースを、STPAによりシステムチェックに導出できるかを確認する。

備考：本例は、人とシステムの競合により発生するかもしれないトラブル例であり、STPAによりシステムチェックに導出できるかを確認するための想定トラブルである。なお、本想定トラブルは実際の製品とは無関係であり、実際の製品では何らかの安全施策が採られていると考えられる。本例は、あくまでも、STPA事例の説明のための想定例である。

- (1) JASPAR機能安全WGの全体活動
- (2) STAMP/STPAチーム活動と事例拡充ガイド概要
- (3) 試行対象システム (自動運転システム)
- (4) STPA試行事例 (自動運転システム)**
- (5) ライフサイクルに対しての試行
- (6) まとめ

第1ステップ： 解析目的を定義

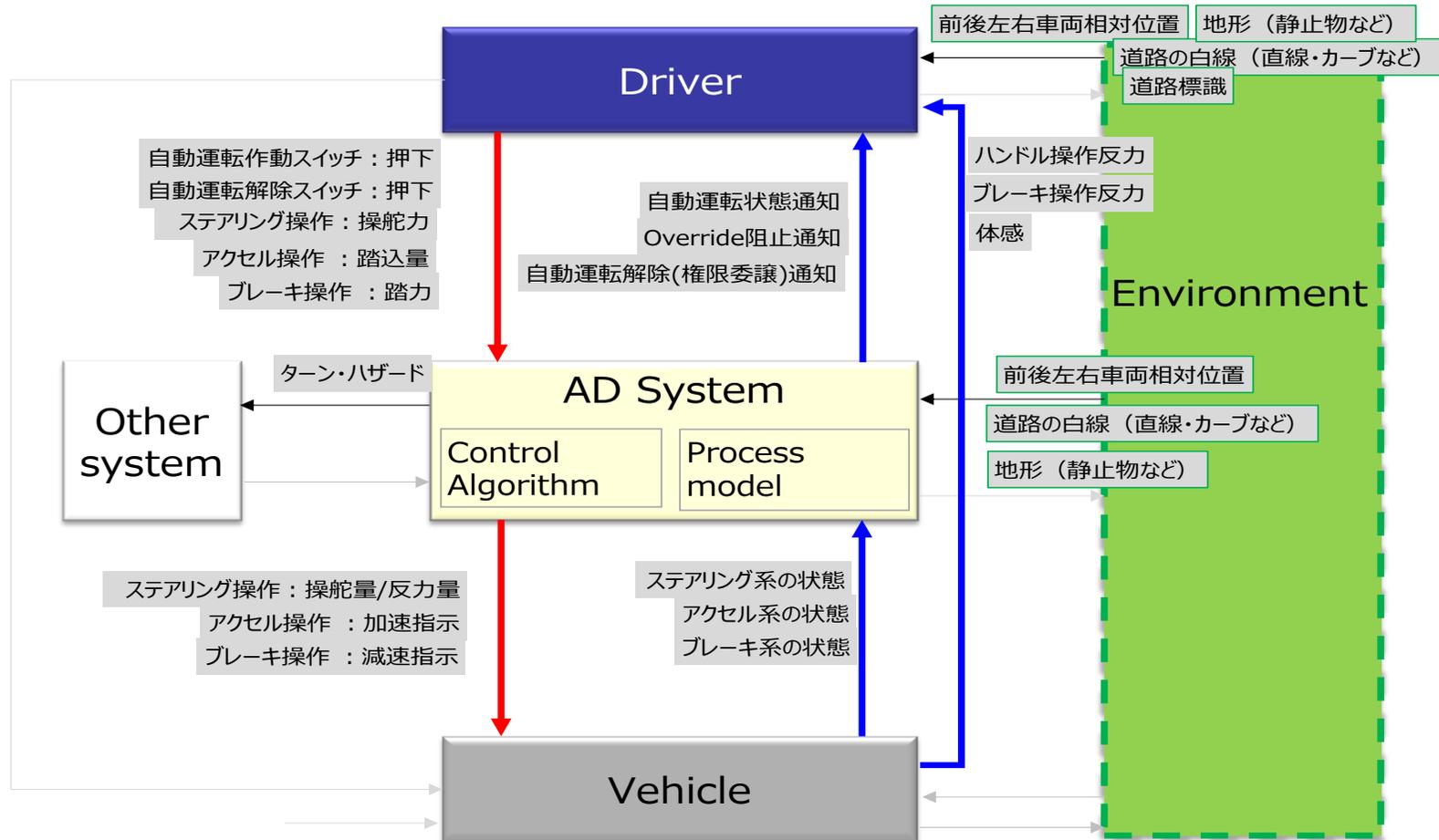
・システム境界の識別とコンポーネントを定義



・損失、ハザード、安全制約(Loss, Hazard, Safety Constraints)を識別

損失 Loss	ハザード Hazard	安全制約 Safety Constraints
他の走行中の車両に衝突する(L-1)	他の車両と十分な車間距離をとらない(H-1)	他の車両と十分な車間距離をとること(SC-1)
周りの静止物に衝突する (路側帯の故障車両含む) (L-2)	周りの静止物と十分な距離をとらない(H-2)	周りの静止物と十分な距離をとること(SC-2)

- ・人／システム／車両／環境をコンポーネントとした車両レベルのコントロールストラクチャを対象としたテンプレートを活用
- ・本事例での分析に関連すると思われるコンポーネント間の相互作用を記入



【備考】 適用するテンプレートは、分析者の立場や分析の目的によって、適切と思われるものを選択してよい。当該ガイドに掲載の各社の分析事例では、異なったテンプレートを選定した場合の例も示されている。

- ・ドライバと自動運転システムの相互作用に着目
⇒ その中でも相互作用の干渉が懸念される自動運転中のオーバーライド機能について非安全なコントロールアクション(UCA: Unsafe Control Action)を分析
- ・3種のControl Actionについて分析
(1)ステアリング操作、(2)アクセル操作、(3)ブレーキ操作
- ・以降の安全分析(ステップ4)の実施後に、振り返り補充する場合もある

ステアリング操作に関するUCA表(抜粋)

No.	CA (Override時)	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Apply too long
CA-1	ステアリング操作	—	ドライバが、高速自動車道で自動運転中に後続車両がいる際にオーバーライドしようと、ステアリング操作を与える。[CA1-P1] ドライバが、高速自動車道で自動運転中にオーバーライドしようと、過剰なステアリング操作を与える。[CA1-P2]	—	ドライバが、高速自動車道で自動運転中にオーバーライドしようと、ステアリング操作を長く与える。[CA1-D1]

- ・[CA1-P2]は、今回注目している想定トラブル事例に該当する。
- ・[CA1-P2]は、後段の分析で識別され、振り返り追記してもよい。

第4ステップ 損失シナリオを識別

想定トラブル例に関連するUCA [CA1-P2] に対する損失シナリオの識別結果

次の理由でドライバが過剰なステアリング操作を与える

(1)自動運転システムによる反力とドライバによるステアリング操作の競合
【ドライバによるステアリング操作の分析】

(1-1)ドライバは反力が自動運転システムによるものとは気づかない
(そのため、過剰なステアリング操作を与える)
・なぜなら、XXX

【自動運転システムによる反力の分析】

(1-2-1)自動運転システムがドライバのオーバーライドを拒絶(自動を優先)して、車線キープした(反力発生)
・なぜなら、自動運転システムは後続車が迫っていると認識した

(1-2-2)自動運転システムがその後、オーバーライドを許可(手動を優先)して、ドライバによるステアリング操作に従った(反力消失)
・なぜなら、自動運転システムは後続車が離れたと認識した

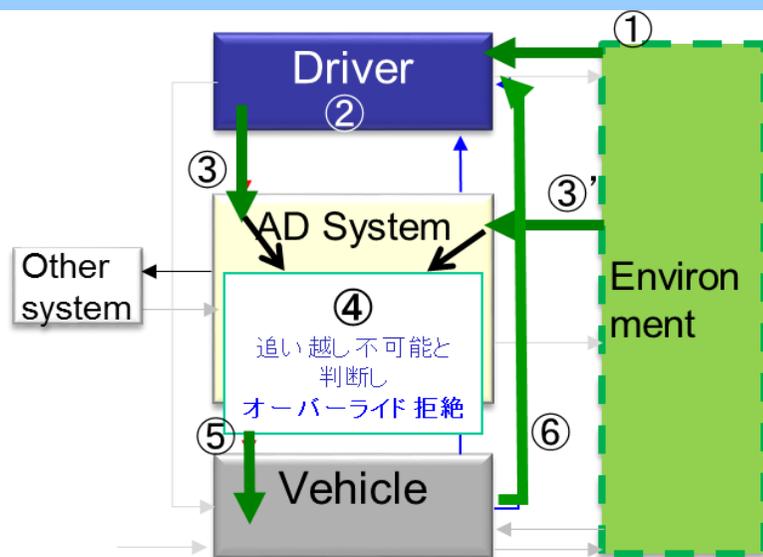
(2)あるいは、XXX
(以下省略)

ヒントワード「コンフリクトするコントロールアクション」から抽出

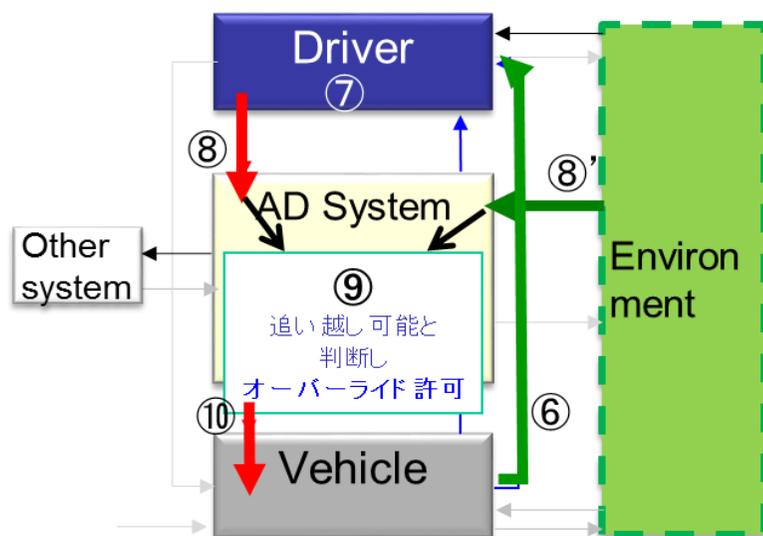
「ドライバのプロセスモデルの矛盾」「フィードバックが不適切」から抽出

コンフリクトするコントロールアクションから「反力発生／消失」を抽出し、そのシナリオを検討

非安全なふるまいの影響順序とループの記述により、損失シナリオを見える化



- ① ドライバが、追いつくために周辺環境(後方車との距離)を認識する
- ② ドライバが、「後方車との安全距離有」と判断し、追いつく可能と判断する
- ③ ドライバが、ステアリング(操舵力)を与える
- ③' 自動運転システムは、周辺環境(後方車との距離)を認識する
- ④ 自動運転システムは、「後方車との安全距離無」と判断し、追いつく不可能と判断し、ドライバーからのオーバーライドを拒絶する(自動を優先する)
- ⑤ 自動運転システムは、車線をキープする
- ⑥ 車両は、ステアリングの舵角をキープするため反力を発生する



- ⑦ ドライバは、反力が「自動運転システムが追いつく不可能と判断してオーバーライドを拒絶している」によるものとは気づかず、オーバーライドのための操舵力が不足していると判断する
- ⑧ **ドライバーは、自動運転システムに対して過剰なステアリング(過剰な操舵力)を与える**
- ⑧' 自動運転システムは、周辺環境(後方車との距離)を認識する→このとき後方車がスピードを下げたため距離増加
- ⑨ 自動運転システムは、「後方車との安全距離有」と判断し、追いつく可能と判断し、ドライバーからのオーバーライドを許可する(手動を優先する)
- ⑩ 自動運転システムは、ドライバーの過剰な操舵力に従って、**車両に対し、過剰なステアリング(過剰な操舵量)を与える**

■想定トラブル事例の抽出

ドライバと自動運転システムとの相互作用によって発生しそうなトラブルを想定し、その想定トラブル事例を、STAMP/STPAによりシステムチェックに抽出できることを確認した。

■テンプレートの活用

JASPARで提唱のテンプレートの中から、人／システム／車両／環境をコンポーネントとした車両レベルのコントロールストラクチャのテンプレートを活用した。

その活用成果は以下である。

- ・車両/システム/人/環境の相互作用に着目した安全分析が明示的にできた。
- ・目的に応じたテンプレートを用いることで抽象度を維持した安全分析ができた。
- ・STPAの初期導入段階でも、テンプレート活用により一定の分析結果が得られる。

今後STPAに慣れてきた場合は、目的に応じてテンプレートをカスタマイズすることで、より効果的な分析が期待できるであろう。

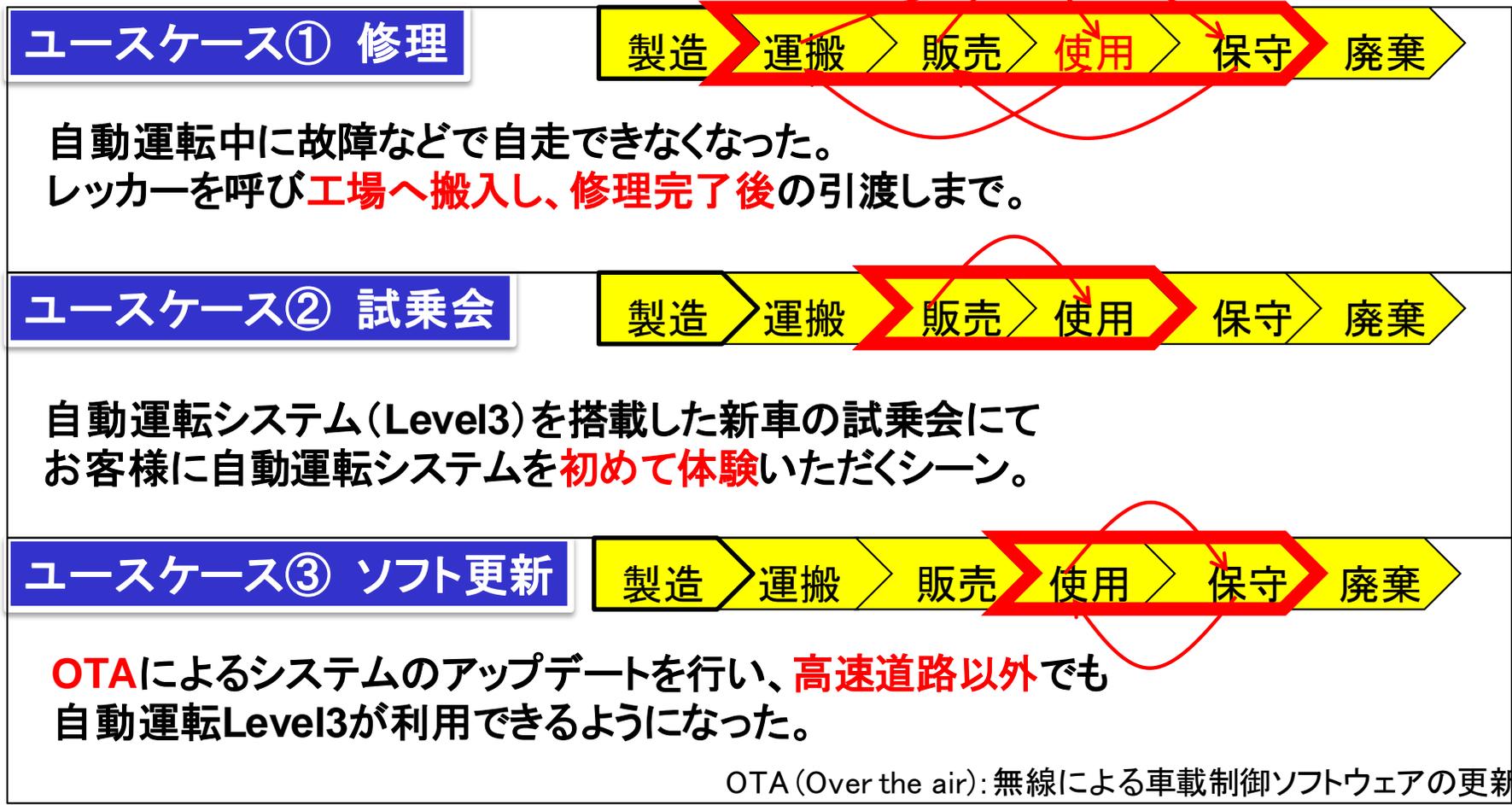
■損失シナリオの見える化

JASPARで提唱の「損失シナリオの見える化」(コントロールストラクチャ上にUCAやそのシナリオを矢印で記載)も適用した。

損失シナリオが相互作用の干渉などによって複雑な場合でも、コントロールフローの視点で整理した説明により、システムチェックにわかりやすく説明できる。

- (1) JASPAR機能安全WGの全体活動
- (2) STAMP/STPAチーム活動と事例拡充ガイド概要
- (3) 試行対象システム (自動運転システム)
- (4) STPA試行事例 (自動運転システム)
- (5) ライフサイクルに対しての試行**
- (6) まとめ

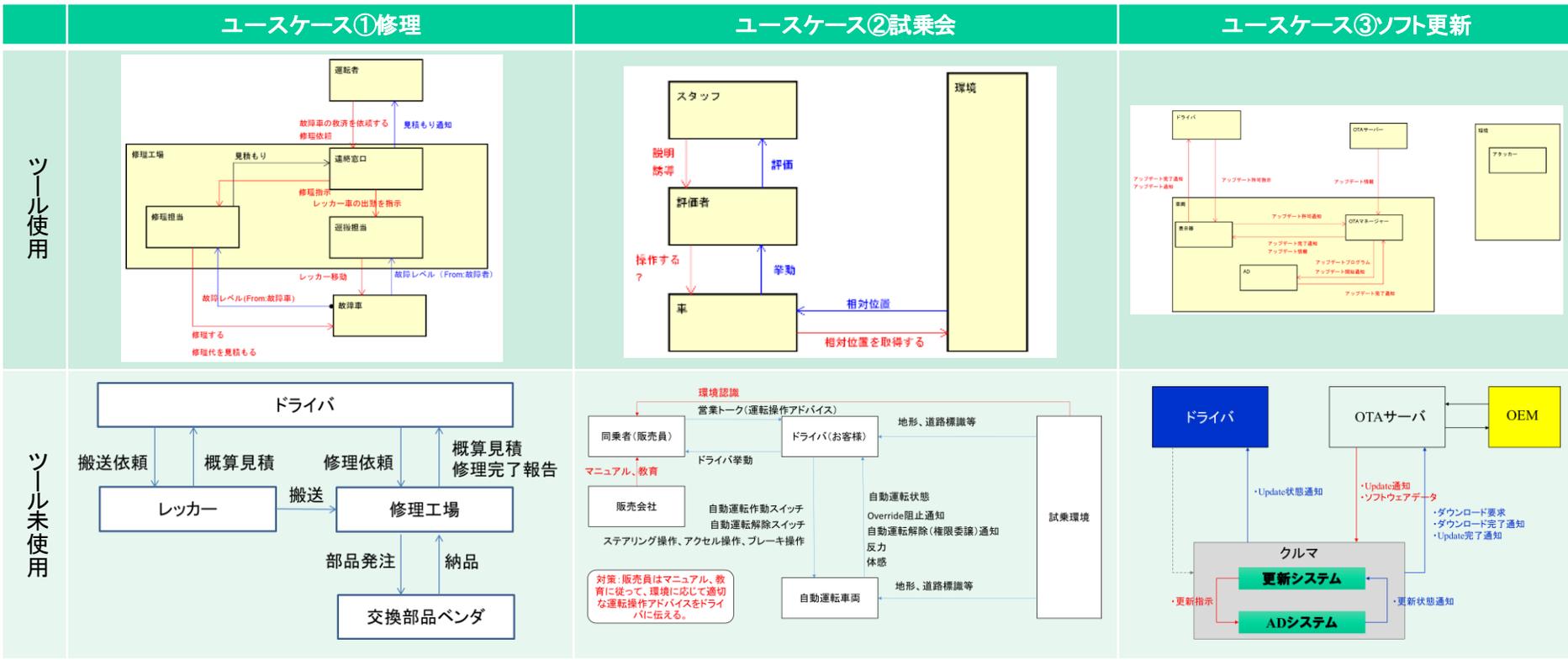
ユースケースを、自動運転の使用段階のみでなく、そのライフサイクルステージに拡充



⇒ 3つのユースケース x 支援ツール使用/未使用 = 6チーム で分析試行

ライフサイクルに対してのSTPA試行

■各チーム(6チーム)で策定したコントロールストラクチャ



■試行による気づき

- ・視点変化によりLoss、Hazard、Safety Constraintsも異なる。(セールス失敗、クルマの紛失、お金・・・)
- ・登場人物の変化→CS図、インタラクションも変わる。(人⇄機械、人⇄人、機械⇄機械、人⇄組織(企業))
- ・CS図は、静的な構造を示すため、各コンポーネント間の時系列変化に対応しにくい
 - シーケンス図・アクティビティ図、状態遷移図などの動的ダイアグラムも併用
- ・試行を通して支援ツールSTAMP Workbenchへの新たな要望やフィードバックが抽出された
 - コンポーネントの分割・集約のサポートなど

- (1) JASPAR機能安全WGの全体活動
- (2) STAMP/STPAチーム活動と事例拡充ガイド概要
- (3) 試行対象システム (自動運転システム)
- (4) STPA試行事例 (自動運転システム)
- (5) ライフサイクルに対しての試行
- (6) まとめ**

- ◆クルマの電子制御化は、自動運転も視野に入れつつ、急速に進化中。自動運転では複数のシステムが連携する大規模かつ複雑なシステムとなる。従来の安全分析(FTA, FMEA)のみでは、検討漏れ、手戻り発生リスクがあり、STAMP/STPAの活用が有効と期待される。
- ◆JASPAR機能安全WGでは、STAMP/STPAを、開発現場で効果的・効率的に活用できないかを検討し、各種事例の試行、活用ガイドの策定、啓蒙活動教材の編集などを行ってきた。
- ◆18年度に追加策定の「STAMP/STPA活用ガイド～自動車 事例拡充編～」では、自動運転システムを対象事例としたSTAMP/STPAの試行を行い、(1)STPAが人(ドライバ)とシステムとの競合の考慮に有効であること、(2)JASPAR提唱の「コントロールストラクチャテンプレート」および「損失シナリオの見える化」の有効性 などを確認した。また、ライフサイクルに対しての試行も行った。

【ご参考】

今回紹介の「STAMP/STPA活用ガイド～自動車 事例拡充編～」は'19年3月に公開予定 (JASPAR会員向け)
(ガイド入手希望される方でJASPAR未加入の場合は、JASPARへのご加入を検討ください)

ご清聴ありがとうございました

以上